Exhibit 1

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213

To: The Commission

DECLARATION OF KIRK CARLSON IN SUPPORT OF THE COMMENTS OF THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION REGARDING THE SCOPE OF CALEA CAPABILITY REQUIREMENTS

1. I, Kirk Carlson, make this declaration on personal knowledge.

2. I am the Executive Director and founder of Synacom Technology, Inc., 3031 Tisch Way #400, San Jose, California 95128. Synacom Technology's main business is systems to support services on intelligent wireless networks.

3. I obtained an SBEE in 1977 from Massachusetts Institute of Technology and have twenty years of telecommunication experience working for TRW Vidar (a manufacturer of digital end-office and tandem switches), Sun Moon Star (a manufacturer of hybrid key telephone systems), and Tandem Telecommunications Systems (a manufacture of intelligent network signaling equipment).

4. My work for Synacom over the past nine years has been to provide consulting services for systems engineering and standards development of protocols for wireless networks. Most recently, I served as editor of what ultimately was published by the Telecommunications Industry Association as J-STD-025, *Lawfully Authorized Electronic Surveillance*. I currently participate in the Enhanced Surveillance Services project of TIA's Subcommittee TR-45.2, which is working to create an industry standard that meets the enhanced surveillance requirements of law enforcement that are not covered in the Communications Assistance for Law Enforcement Act ("CALEA").

5. Attached to the Cellular Telecommunications Industry Association Comments Regarding the Scope of CALEA Capability Requirements, the Commission will find a letter from the Subcommittee Chair to Mike Warren, CALEA Implementation Section, asking for a clear and definitive statement of law enforcement requirements for the ESS. The enclosures to the letter illustrate the degree of ambiguity, technical imprecision and overbreadth in the FBI's proposed requirements for additional CALEA features. Law enforcement has been asked to respond to the submission by the next ESS meeting in mid-June.

6. In addition, for purposes of this proceeding, I have reviewed the Department of Justice and the Federal Bureau of Investigation Joint Petition for Expedited Rulemaking filed with the Federal Communications Commission on March 27, 1998. I particularly reviewed Appendix 1 of the Joint Petition. As an expert in the telecommunications field and as editor of J-STD-025, I have numerous concerns with the technical merit, the breadth of the document, and its severe impact on, and compatibility with J-STD-025. To assist the Commission in understanding the problems with law enforcement's proposed rule, I have prepared the enclosed annotated copy of the proposed rule.

Dated this 20th day of May, 1998.

Kirk Carlson

***CARLSON COMMENTS APPEAR AS INDENTED MATERIAL**

APPENDIX 1 - Proposed Final Rule[1]

AMENDMENTS TO THE CODE OF FEDERAL REGULATIONS

PART 64 - MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Part 64 of Title 47 of the Code of Federal Regulations (C.F.R.) is amended as follows:

1. The authority citation for Part 64 is modified to read as follows:

AUTHORITY: 47 U.S.C. §§ 151, 154, 201, 202, 205, 218-220, 229, 332, and 1006 unless otherwise noted. Interpret or apply §§ 201, 218, 225, 226, 227, 229, 332, 48 Stat. 1070, as amended, 47 U.S.C. §§ 201-204, 218, 225, 226, 227, 229, 332, 501, 503, 1002, and 1006 unless otherwise noted.

2. The Table of Contents for Subpart Q of Part 64 is amended to add Section 64.1706 to read as follows:

§ 64.1706 Electronic Surveillance Standards
§ 64.1707 Interim Standard J-STD-025 Assistance Capabilities
§ 64.1708 Additional Assistance Capabilities

3. New paragraphs are added, in alphabetical order, to Section 64.1702 to read as follows:

§ 64.1702 *Definitions.* * * * For purposes of Sections 1706 through 1708 of this Part, except where otherwise noted herein, terms defined in Interim Standard TIA/EIA/IS-J-STD-025 ("J-STD-025") shall have, respectively, the meanings stated in that document.

The definitions in this section appear to be modifying the definitions in J-STD-025 by rule. In general changing the definitions used to develop a standard will require that the standard be reviewed, modified and re-balloted to ensure that it is consistent and aligned with the new definitions.

Access: Means the technical capability to interface with a communications facility, such as a communications line, switch, or other network element so that a law enforcement agency can receive and monitor call-identifying information and call content.

This is a slight modification of the J-STD-025 definition that should have little or no impact.

---

[1] This draft proposed final rule follows the formatting of the Commission's proposed Final Rule in the pending rulemaking proceeding *In the Matter of the Communications Assistance for law Enforcement Act,* CC Docket No. 97-213 (released October 10, 1997).

Assistance Capabilities: Means the electronic surveillance services and features provided by carriers to law enforcement pursuant to Section 103 of CALEA, 47 U.S.C. §1002, and as defined by rules promulgated by the Federal Communications Commission.

By referring to the FCC rules, the capabilities must be extended over those defined in Section 103 of CALEA. This provision may complicate the interpretation of a standard, such as J-STD-025, since it may no longer be a stand alone document.

Call: Means a sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used, as defined in J-STD-025. A call may have one or more legs.

Call Appearance: Means an instance of a call or call attempt with direct subject control, as defined in J-STD-025. For example, a party with three call appearances may be involved in and control three calls simultaneously. Some services that do not permit the subject to directly control the call, such as call forwarding, do not consume [use up] call appearances.

This is a modification of the J-STD-25 definition that may have a profound impact. A call appearance is not an instance of a call attempt. It is only an instance of a call. It is created when resources are required for a call, but not necessarily for a call attempt. The distinction here is fine. An attempted outgoing call does not become a call until facilities are seized and that may be delayed until the call attempt is authorized and a route is selected. When an incoming call arrives and there are no call appearances available for the called party, the call will be given busy treatment.

Call Content: Means, when used with respect to any wire or electronic communication, any information concerning the substance, purport, or meaning of that communication, as defined in 18 U.S.C. §2510(8), and includes any transfer of messages, signals, writing, images, sounds, data, or intelligence of any kind by or to a subject.

While an electronic communication can be "any transfer of signs, signals, writing,, images, sounds, data, or intelligence of any nature," call content is limited to the "substance, purport, or meaning of that communication." So the electronic communication itself need not be intercepted, only the substance, purport or meaning of that communication. Without this interpretation the intercept would have to be the actual communication without modification. Wireless intercepts could only be delivered in an unmodified wireless format. If the communication used audio carried by FM radio waves, we would have to deliver audio carried by FM radio

waves. Clearly this is not workable using normal telecommunication systems. Telecommunication service providers may change the format of the communication as long as the substance, meaning and purport are preserved. J-STD-025 follows that lead and allows content to be delivered using a standard or widely available protocol.

Additionally this redefinition of call content would require all of the signaling used to control the subject's communications to be sent as well whether that signaling was to control a subject's access terminal, intersystem signaling to negotiate the subject's services, network signaling to establish and control communication, or messages used to manage and account for use of the network resources used by the subject. At the same time messaging that is not authorized, such as the messaging for information services, would have to be excluded.

J-STD-025 would have to be modified extensively to handle this re-definition. This single change may be very expensive, because it dramatically increases the amount of signaling information that would have to be delivered to law enforcement.

Call Content Channel (CCC): Means the logical link between the device performing an electronic surveillance access function and the law enforcement agency that primarily carries the call content passed between a subject and one or more associates, as defined in J-STD-025.

Call Data Channel (CDC): Means the logical link between the device performing an electronic surveillance access function and the law enforcement agency's collection equipment that primarily carries call-identifying information, as defined in J-STD-025.

This slight rewording of the J-STD-025 definition has little technical impact other that to place a requirement on the telecommunication service provider beyond the point of demarcation (i.e., to the collection equipment and the intervening transmission equipment, facilities, or services) for the CDC

Call Forwarding: Means any of the several features that redirect a call to another directory number (or voice mail) if a certain condition (or set of conditions is met), as defined in J-STD-025.

Call-Identifying Information: Means all dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subject

by means of any equipment, facility, or service of a telecommunications carrier, as defined in CALEA Section 102(2), 47 U.S.C. § 1001(2).

This appears to redefine "call-identifying information" by being one of the few definitions that is not referenced to J-STD-025. J-STD-025 takes its definition for call-identifying information from the law and then defines the four terms that caused confusing and contention. These words are "origin," "direction," "destination," and "termination" as the terms are understood in the industry.

Call Leg: Means a bi-directional call path associated with each network facility usage attempt and subsequent usage, as defined in J-STD-025.

Circuit: Means a switchable bi-directional path between two locations, as defined in J-STD-025. A circuit may be all or part of a channel. On an end-to-end circuit, separate physical facilities may be used for each segment of the circuit.

Circuit-Mode: Means a communication using bi-directional paths switched or connected when the communication is established. The entire communication uses the same path.

Communication: Means any wire or electronic communication, as defined in 18 U.S.C. § 2510.

Complete: Means a call attempt that is answered.

Connection: Means a relationship between two or more parties of a call to allow communication between them.

Cut Through: Means the completion of a connection in one direction (partial), or both directions (full), between two call appearances.

This is nearly as it was defined in J-STD-025, except that add the phrase "between two call appearances." This is normally true, but not necessarily true. Cut-through occurs upon answer, but it occurs on a switch by switch basis. One switch at one end of the call may not cut-through the call (such as post-pay coin phones or in some collect calling scenarios), but other switches involved in the call are cut-through. There is no network indicator for the end-to-end cut-through of a call.

Demarcation Point: Means the point separating the telecommunications carrier's facilities from government-procured delivery facilities and is the point at which a telecommunications carrier transfers the intercepted call content and call-identifying information to the law enforcement agency.

Intercept Access Point (IAP): Means the point at which a telecommunications carrier accesses communications or call-identifying information.

This re-definition may require that all accesses be performed at a single point for a given subject. That is not possible with modern distributed systems, especially for wireless systems and intelligent networks. J-STD-025 envisioned that a subject's communications would have to intercepted by several IAPs in several systems with each IAP accessing only part of the intercept subject's communications.

J-STD-025 also required the IAP to be within a telecommunication system. This redefinition implies something more ominous by monitoring communications externally to a telecommunication system.

Interface: Means the format defining the information to be exchanged, and the procedures for generating, sending, receiving, and processing that information, that must be selected and used by both parties in order for communications to take place between a telecommunications carrier's network and a law enforcement agency's equipment. The Open Systems Interconnection (OSI) Reference Model of the International Telecommunications Union (ITU) provides a common language describing the sequence of hardware or software protocols (i.e., the protocol stack) that must be used by the Interface to enable communication.

Many standards, including J-STD-025, specify interfaces only to the extent necessary for the interfaces to be used. This allows an application layer protocol to be in a variety of ways with different delivery media. It is not necessary to specify any and all envisioned situations and then modify when something new comes along or when unforeseen situations arise. This flexibility makes that standard more cost effective and better able to meet future situations.

J-STD-025 is not an interface specification, nor was it ever intended to be. It is an application layer protocol specification. It may impossible to define all of the protocols that will be delivered over the CCC as requested herein at §64.1708 (j) because the industry is constantly adding new telecommunication services. At the same time the user community is adding new protocols to use the existing services with a rich variety of modems, faxes and data protocols, such as X.25 or the internet suite of protocols. Delivering a CDC to law enforcement using only X.25, as they have requested in the past, may require will over 5 protocol stacks to deliver the information using only traditional analog lines and digital lines.

Of and by itself this definition is harmless, but what it implies has a profound effect.

Subject: Means a person who uses telecommunications equipment, facilities, or services that are subject to a court order or other lawful surveillance authorization, and whose communications or call-identifying information are intercepted and delivered to a law enforcement agency.

This redefinition serves only to complicate the issue by separating the intercept subject from the investigative target. J-STD-025 defines the intercept subject as the subscriber whose equipment, facilities, or services are subject to intercept. J-STD-025 does not separate the intercept subject from the subscriber. To do so, as has been done with this proposed final rule, shows that the two are to be treated different and that new capabilities are introduced to intercept the investigative target's communications rather than those of the intercept subject. This is especially true if it is necessary to identify and isolate the investigative target from any number of associates of the intercept subject. (Surely the proposed rule does not presume that all call associates are to be treated as investigative targets.)

Expanding this definition requires expanded capabilities. It may require revising J-STD-025 to ensure that consistent and legal treatment is applied throughout the document.

Subscriber: Means the person or entity whose telecommunications equipment, facilities, or services are subject to a court order or other lawful surveillance authorization providing that the communications or call identifying information, or both, carried by that equipment, or supported by those facilities or services, are to be intercepted and delivered to a law enforcement agency.[2]

This is the intercept subject in J-STD-025 and should not be redefined. See Subject.

---

[2] The term "Intercept Subject" is defined in J-STD-025 as the "telecommunications service subscriber whose communications, call identifying information, or both, have been authorized by a court to be intercepted and delivered" to a law enforcement agency. As a legal matter, however, a court order or other lawful surveillance authorization under 18 U.S.C. §§ 2510-2522 (content), or 18 U.S.C. §§ 3121-27 (call-identifying information), applies to the telecommunications equipment, facilities, or services under surveillance, not to the communications of a specific individual. 18 U.S.C. § 2518(4)(b); *id.* § 2518(1)(B)(ii). Section 64.1708 of this Part therefore does not adopt the "Intercept Subject" nomenclature used in J-STD-025. The term "Subscriber" is used in Section 64.1708 to identify to identify the person whose telecommunications equipment, facilities, or services are under surveillance. The term "Subject" is used to identify the parties whose communications and call-identifying information are intercepted and delivered to a law enforcement agency; these parties may include the Subscriber (as that term is defined herein), or other persons who use the Subscriber's telecommunications equipment, facilities, and services.

Both CALEA and J-STD-025 focus the intercept capability on telecommunication service subscribers.

Even here there may have been an attempt to define the intercept subject as a person rather than as a subscriber. The technical difference between these two is great. Switching systems maintain information about their subscribers, not about the persons or places that these subscribers may be calling. Switches also do not maintain information about casual users, such as pay phone callers.

Telecommunications Carrier: Means "telecommunications carrier," as that term is defined in CALEA Section 102(8), 47 U.S.C. § 1001(8).[3]

4. Sections 64.1706 through 16.1708 are added, to read as follows:

§ 64.1706 *Electronic Surveillance Standards.* Telecommunications carriers shall comply with the assistance capability requirements set forth in Section 103 of CALEA, 47 U.S.C. §1002. In order to comply with these assistance capability requirements, telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the electronic surveillance assistance capabilities defined in the electronic surveillance interface standards set forth in Sections 64.1707 through 64.1708, below.

§ 64.1707 *Interim Standard J-STD-025 Assistance Capabilities.* Telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the electronic surveillance assistance capabilities defined in the electronic surveillance interface standards set forth in Interim Standard J-STD-025, TIA/EIA/IS-J-STD-025, (December 1997), published jointly by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS). This incorporation by reference was approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies of the document may be inspected at the Federal Communications Commission, 1919 M Street, NW., Washington, DC 20554 or at the Office of the Federal Register, 800 N. Capitol Street, NW., Washington, DC. Copies of J-STD-025 can be obtained from the Commission's contract copier or from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5704 (1-800-854-7179) or the Alliance for Telecommunications Industry Solutions, 1200 G Street, N.W., Suite 500, Washington, DC 20005 (202-628-6380).

While J-STD-025 was carefully written with a wide variety of communication services in mind, it would be wrong to think that only J-STD-025 could satisfy the CALEA requirements or that it can do so even as modified by this proposed rule. Different technologies, products and services may require

[3] The Federal Communications Commission is also addressing the definition of "telecommunications carrier" in the pending rulemaking proceeding *In the Matter of the Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213 (released October 10, 1997).

different solutions. The ultimate decision for the applicability of any solution rests with the telecommunication service provider and its equipment vendors. TIA standards are voluntary in that they can be implemented in whole or in part by any one who chooses to do so. They can use other options. Even law enforcement has stated that plain old telephone services (POTS) could use the existing methods for electronic intercept. Since J-STD-025 does not define existing intercept equipment, adoption of this paragraph would render that equipment non-compliant. This would have a large cost impact to telecommunication service providers and law enforcement.

§ 64.1708 *Additional Assistance Capabilities.* In addition to the assistance capabilities defined in J-STD-025 and referenced in Section 64.1707, above, telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the following additional electronic surveillance assistance capabilities:

(a) *All Content of Conferenced Calls.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing to law enforcement all content of conferenced calls over a subscriber's equipment, facility, or service, where capability is defined as the ability to monitor a multiparty or conference call established by the subscriber's equipment, features, or services where two or more parties are allowed to converse after the subject leaves the conversation, temporarily or permanently.

This requirement is a little confusing as written because of the secondary clause. One way to read this is that separated delivery of each party of the conference call is required, a long-time favorite capability for law enforcement. This reading comes about from the use of the word "all." On the surface this could mean all of content of a conference call, which may be slightly different for each party, therefore requiring separated delivery of each party. The secondary clause attempts to refine this interpretation, but it only restricts the capability to a conference call where the intercept subject leaves the call and the remaining parties are allowed to converse. At a minimum the word "all" should be removed.

A conference call works by selecting or combining the inputs from the participating parties and presenting the selected speech back to the participants. In most conference services what each party hears is technically and mathematically

different, because the party's own contribution to the conference service does not contribute to the output to that party. Furthermore some input from some parties may be discarded. Even though what is delivered to each party may technically be different, the meaning purport and substance is the same for all participating parties. For example, a conference circuit may select the loudest two speakers at any point in time, combine the speech from those two speakers, and present the result to all of the participants of the conference. Individual inputs may be discarded, when discarded, they are not part of any communication, since they were not delivered to another party: no communication took place. However, the meaning, purport and substance of the communication is carried by the selected and combined output. The content can be obtained by monitoring any leg of the conference call. The leg toward is the intercept subject is the most convenient place to intercept that content. However that leg may not always be present, when the subject leaves the conference. Requiring the leg may be detectable to other participants of the conference call with some conference circuits.

This also seems to place the requirement on the access service provider and not on the service provider offering the conference service. There should be no requirement to access a held conference call if the call is not held by the service provider with the court order.

This requirement may be incomplete, if it is to be consistent to monitor a service such as meet-me conference where the intercept subject may never be a party to the conversation and may not be a subscriber of the service. Note however that applying capabilities specifically to meet-me conference and certain other features that are used on a one-time or demand basis may require a complex and expensive solution. The solution is complicated by the fact that meet-me conferences are often provided by independent third parties rather than a telecommunication service provider.

(a)(1) For subject-initiated multiparty calls, multiple CCCs may be necessary if the subscriber's service will support communications with two or more associates. CCCs shall follow the subscriber's terminal. A separate CCC shall monitor the subscriber's conference service when the subject is separated from the subject's conference. Call content shall be delivered to law enforcement

whenever the subscriber's service continues to support the communications of the associates.

This requirement is a masked capacity requirement not a capability requirement. CALEA separates the two and provides for separate treatment. Furthermore this requirement is not necessary. J-STD-025 has the requirement to monitor multiple call appearances as long as there are CCCs available to deliver content. CCCs are assigned on as needed basis and therefore would follow the conference call and not necessarily the intercept subject's new service attempt. Call content be will be missed if there are not enough CCCs to deliver the call content. Some priority had to be applied, and first-come, first-serve seemed to meet other law enforcement requirements, such as not dropping any part of an intercepted communication. Changing this priority scheme will be costly to manufacturers and may be confusing to law enforcement.

(a)(2) On a subject-initiated multiparty call, call content shall not be delivered over the CCC when the subject leaves the multiparty call and only one party remains on the multiparty call.

This requirement is little ambiguous as written. If a call is placed on a temporary or soft hold to initiate a three-way or conference call, this requirement would prohibit the delivery of call content of the held associate. However, it does not specify the treatment if a hard hold is used during a two-party call with an associate. It does not specify the case where are of the parities of a multi-party hold are separately placed on hold. Logically these two cases are the same from a switch point of view, so the requirement should be to not deliver call content for any single party placed on hold or more generally to not deliver call content unless the accessed party is able to communicate with another party.

A requirement similar to this was proposed for J-STD-025, but was not adopted. Part of the industry argument centered around the ease of turning off the monitoring. It may simplify implementations to allow the contents of a held party to be delivered. Law enforcement's argument was to not preclude the delivery of content of the held calls. J-STD-025 is silent on this issue: the delivery of the held portion of calls is neither required nor prohibited, but is left to implementation.

(b) *Party Hold, Party Join, and Party Drop Messages.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable

of providing messages to law enforcement that enable law enforcement to identify the parties to a conversation at all times.

This paragraph seeks to extend the definition of a communication into a set of one or more "conversations." Telecommunication service providers do not keep any records of conversations, nor is there normally external signaling generated by every change of conversation within a communication.

For example, if a call is made, placed on hold and then retrieved from hold, law enforcement would like to be informed of the conversation transitions within that call. The communication, as far as the service provider is concerned is the entire time between the request for facilities and the release of those facilities (see definition of call). Nothing is normally recorded or reported for placing a call on hold by a telecommunication service provider or its equipment. A more complex case is call waiting where a subscriber toggles back and forth between two parties. Depending on the implementation, this may be treated as two separate calls similarly to the first example. Alternatively the case could be treated as a single call where one party is placed on hold and then the other party is retrieved from hold. In either case the conversations for the two other parties are recorded as their entire duration, irrespective of any time on hold.

A connection-oriented packet-mode communication consists of three phases: setup, data transfer and release. We have viewed CALEA as requiring reporting of the setup phase to identify the origin, destination, direction and termination of the communication. J-STD-025 reports on the setup and the release phases. With a broad interpretation of this requirement, it would also require information during the data transfer phase to report individual packets during the data transfer phase and to report the mixing of data transfer packets from different communications.

Another extreme, but possible, interpretation of this requirement is to report the speaker selected by a switching conference circuit (a typical method for conference services with over three parties). This would require getting into a piece of dedicated hardware and generating messages. In some cases several messages may be generated per second.

While this capability may be fairly easy to implement on some systems, it may be because these systems have a

simple feature set. On more advanced systems, and certainly on more future systems, the feature sets are more complex and this capability becomes more complex. Because this feature requires instrumentation to be inserted into the call processing code to detect and report the transitions, this capability increases the amount of processing for every call, whether the parties involved are under surveillance or not. This translates into either lower switch capacities for a given implementation or a requirement for more processing power. Either of these results in higher costs for systems, even if surveillance is used.

The capability does nothing to identify the human participants or participation in calls. Simply reporting the connection state of a particular switching system does not imply that the communication reaches the distant party nor does it imply that the party hears the rest of the communication. Connections may be affected by the services and features of other parties as well as the customer premises equipment of all parties (e.g., to put a call leg on hold, transfer the call leg to another party, or to conference in a group of people). More simply someone may lay the telephone receiver down to answer the door. On top of that the identifiers may at best identify a particular terminal, but they cannot identify a particular person. The only way to verify a communication is to identify the voices participating in that communication including any response to verify that something was heard.

At a minimum this feature should only apply to full Title 3 intercepts and not to pen registers and trap and trace orders, because with out the call content, the identifiers provide nothing beyond that already provided by J-STD-025.

The text itself is a simple statement of requirement, however it is overshadowed by the description of the capability which dictates that only a prescribed set of messages be used to implement the capability. This needlessly precludes a proposal for reporting the parties with a single message or another proposal for modifying the use of an existing J-STD-025 message. Toggling parties with call waiting would require at least two messages with this proposal rule: one to place a party on hold and one to retrieve a party from hold. A single message identifying the current parties may be sufficient to satisfy the basic requirement.

(b)(1) *PartyDrop.* The PartyDrop message reports when one or more parties to a call are released and the call continues with two or more other parties. The PartyDrop message shall be triggered and delivered when a party is released from a multi-way call (e.g., three-way calling, conference call, meet-me conference). The PartyDrop message shall not be triggered when an entire call is released, which is reported by the Release message.

The first sentence is incorrect and does not reflect our understanding of its intent. This would require reporting only when a call has four or more parties, so it would not apply to three-way calling. Fix the intent of the sentence by replacing "two or more other parties" with "at least one other party."

This requirement should be simply to report when a party leaves a communication permanently. This is already supported by J-STD-025 when separate call identities are used for each leg of a call (the normal case for today's switches).

(b)(2) The PartyDrop message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 1: PartyDrop Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
One of Released Party Identities Remaining Party Identities	M	 Identifies parties released from the call. Identifies parties remaining in the call.

This requirement states in effect that only this message can be used and to change the message in any way will require

changing the final rule. As such, it is an over specification of a requirement.

(b)(3) The PartyDrop message shall adhere to the following ASN.1 syntax definition:

```
PartyDrop :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when
the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
    CHOICE {
releasedParties[4]    SEQUENCE OF PartyIdentity,
remainingParties      [5]     SEQUENCE OF PartyIdentity } }
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(b)(4) *PartyHold.* The PartyHold message reports the placing of one or more parties of a call on hold by the subject. The PartyHold message shall be triggered and delivered when one or more parties are no longer connected to a call through use of one of the following features: (i) call hold; (ii) call waiting; (iii) three-way calling; (iv) conference call or meet-me conference; and (v) other similar features or services.

The second sentence is not exactly correct. A call may or may not have connections when a party is placed on hold. A party placed on hold is normally still associated with the particular call and such association may be considered to be a connection. Also in practice it is not technically possible for the intercept subject to place a meet-me conference on hold and have that conference monitored, because it would appear as a two-party held call to the accessed switch. The intercept subject may leave the meet-me conference call and return like any other party to the call. Additionally the meet-me service may allow for taking the subject out of the conference for consultation. This is effected though the service controls, not necessarily the direct intercept subject's control.

Requirement (b) states that it only wants the identifications to parties of a conversation. So this requirement should be simply to report when a party temporarily leaves a communication.

(b)(5) The PartyHold message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 2: PartyHold Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
One of Held Party Identities Remaining Party Identities	M	 Identifies parties placed on hold. Identifies parties remaining in the call.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(b)(6) The PartyHold message shall adhere to the following ASN.1 syntax definition:

```
PartyHold :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when
the
        -- underlying data carriage does not imply that system.
        [3]     CallIdentity,
    CHOICE {
heldParties         [4]     SEQUENCE OF PartyIdentity,
remainingParties    [5]     SEQUENCE OF PartyIdentity } }
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(b)(7) *PartyJoin*. The PartyJoin message reports the addition of a call party to an active call or the retrieval of a held call by the subject. The PartyJoin message shall be triggered and delivered when (i) one or more previously held associates are added to the current call (e.g., call waiting, three-way calling, conference calling) and (ii) an associate joins an existing call with a subject (e.g., barge-in).

The second sentence is not exactly correct because it does not include the case where it is the intercept subject that is joining the call especially if associates are allowed to converse without the intercept subject as proposed in (a).

Citing barge-in as a specific example is especially troubling as this feature is very esoteric and usually extremely complex. Implementations of barge-in may violate normal call processing to provide an emergency capability intended to be used only by operators. Even where systems allow barge-in to be a subscription feature, its use is very limited and it is similar to customer premise equipment (CPE) services offered transparently by PBXs and key systems.

The barge-in reference also could be taken to be a requirement to inform law enforcement when ever a communication under surveillance is accessed in any way. This could include service monitoring features which are periodically used to monitor the quality of service on subscriber facilities or even when an equipment installer uses a telephone test set to access a subject's line. Such

reporting requirements are not reasonably available and may not even be technically feasible.

Requirement (b) states that it only wants the identifications to parties of a conversation, so this requirement should simply to report when a party joins a communication. This is supported by J-STD-025.

(b)(8) The PartyJoin message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 3: PartyJoin Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber. With the redefinition of subject and subscriber, there was a re-definition of CaseIdentity from its source in J-STD-025.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Joined Party Identities	M	Identifies parties that joined the call.

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(b)(9) The PartyJoin message shall adhere to the following ASN.1 syntax definition:

```
PartyJoin :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity              OPTIONAL,
        -- Include to identify the system containing the IAP when
the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
joinedParties   [4]     SEQUENCE OF PartyIdentity}
```

This requirement states in effect that only this message can be used and to change the message in any way will require changing the final rule. As such, it is an over specification of a requirement.

(c) *Subject-Initiated Dialing and Signaling.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing law enforcement with access to all subject-initiated dialing and signaling, including the use by a subject of flash hooks, feature keys, and all other key usage.

Including "all...signaling" is unbounded and could include terminal controls, service control, and network controls, that may have little to do with the communications authorized to be intercepted. CALEA restricts the requirement to delivering only the content of a subject's communications and call-identifying information for those communications. There is some question as to whether signaling issued by a subject to control another's service is even authorized to be intercepted: it is not a communication and it does not identify a subject's communication.

Some keys are not transmitted by the intercept subject's terminal, such as a program key. Other keys are transparently translated by the intercept subject's terminal into a string of signals, such as a speed dial key which is expanded into a normal dialing sequence. In some systems the system will screen controls for which the subscriber is not authorized. That is, if the intercept subject is not authorized for any feature that uses a flash, the flash may not be processed beyond the basic line card for the intercept subject. In these cases, the accessing system is not aware of the intercept subject's dialing or signaling. To gain access to these controls would require architectural changes.

This capability should be limited to the reporting of subject-initiated dialing or signaling that effects the subject's call processing control. However, in many cases such reporting is redundant with other messages. These messages report the effect to call processing, not necessarily what caused the changes to occur.

If the requirement remains to report "all" signaling, it is likely that the signaling will be delivered to law enforcement in its native format and not reprocessed for their convenience. This will greatly increase the cost of law enforcement collection equipment, because this equipment will have to

include the functionality of signal protocol analyzers for several network, access, and wireless air interface signaling protocols. This goes against their requirement stated in (j).

(c)(1) For all subject-initiated dialing and signaling, a message shall be triggered and delivered, which message may be the origination message, that reports subject inputs of flash hooks and other key usage signaled to the network through the use of the following triggers: (i) when a switchhook flash or its equivalent is detected and (ii) when a key press signaled to the network is detected.

This requirement is much more restrictive than (c) and may even be able to be implemented.

(c)(2) The nature of number and presentation/restriction indicators parameters signaled with a telephone number shall be reported in the Context [18] sub-parameter of the PartyIdentity parameter, as defined in J-STD-025.[4]

This requirement is almost never associated with subject initiated dialing as these messages usually interpret the dialed number in the context of the network dial plan and numbering plan. In other words a telephone instrument does not know that it is making an international call and is unable to mark the nature of number. The dialed number indicates that it is an international call with an international access code (011 in the US). These indicators do pertain to identifying parties to incoming calls. (The presentation restriction indicators apply only to calling party identifier and to the redirecting party identifier.)

(c)(3) Origination messages as defined in J-STD-025 shall also be triggered and delivered when the subject goes off-hook without dialing (with a corresponding Release message sent when the subject goes back on-hook).

This requirement begs the definition of a call. It is an incomplete call attempt at best. No communication, in the legal sense, took place. There was no called party to identify. As a call, it never happened. There is no requirement that the switching system be aware that a

---

[4] The "nature of number" and "presentation/restriction indicators" parameters signaled with a telephone number are referred to in the discussion of party identity features contained in ITU-T *Number Identification Services*, ITU-T I.251, at §§ 251.3 ("Calling Line Identification Presentation") and 251.4 ("Calling Line Identification Restriction").

subject is starting a call request. Wireless systems and ISDN get around this requirement with intelligent terminals and some traditional wireline switch hide this information in line cards or in remote switching system. In these cases the central switch is not aware of the event. This requirement forces a design on current and future systems.

(d) *Notification Messages for In-band and Out-of-band Signaling.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing notification messages to law enforcement over the CDC of in-band and out-of-band signaling from the subscriber's service throughout each call. Notification messages shall be triggered and delivered to the law enforcement agency to report out-of-band signaling delivered through a subscriber's service that can be sensed by the subject and to report in-band signaling applied by the equipment, facilities, or services supporting the subscriber's terminal.

Law enforcement may have been getting call progress tone information as a side benefit of dialed number recorders (DNRs). Over the years the functionality of DNRs was expanded beyond the simple recording of the dialed dial pulse or DTMF digits into detecting and reporting of various call progress tones.

Some modern telephone systems now apply some of these call progress tones from the terminal itself using an out-of-band signal. However, traditional in-band call progress tones are still supported to interwork with older network equipment.

The difficulty of this requirement is that, as it is stated, requires a full time tone detector to monitor each communication being intercepted. Presumably this would have to occur for pen registers, which constitutes the vast majority of intercepts. This requires that the communications be intercepted and brought to a specialized tone detector. This detector is specialized in that it can detect the call progress tones. Normally telephone switches are concerned only with detecting tones representing digits (and even then only at the call setup phase of a call).

Intercepting the out-of-band messaging is also problematic to access the signaling that is applied to the terminal requires unusual architectural considerations. This same concern would apply to intercepting the internal commands to cause tones to be applied by the accessing system.

This requirement was made more confusing with the re-definition of the word "subject" to be an investigative target.

This requires that out-of-band signaling that can be sensed by the target would need to be reported, regardless of where the target is (remember that the target may be an associate with the redefinition).

The out-of-band signaling reporting requirement goes far beyond the obvious simple statement. It includes any terminal control, such as power control, that can be sensed regardless of how indirectly. It included may signals sent toward associates that may be sensed by other parties of the call provided that the other parties have a particular network configuration and have a terminal that uses the signal.

The in-band signaling reporting requirement seems intended to only apply to tones applied by the accessing system, but the wording can be interpreted to include any tone applied toward the intercept subject's terminal regardless of where the tone was applied (or during any part of a communication). Reporting tones from distant systems is difficult, because some systems, especially systems in other countries, use different tone plans.

(d)(1) The Notification message shall be triggered and delivered when the accessing system applies an in-band audible indication to the subscriber's receive content channel or sends or passes a command to the subscriber's terminal to activate, deactivate, or control generation of the following indications of incoming calls or messages:

This is the first mention of requirements on incoming "messages." It is not exactly clear what is meant here. This could mean packet data messages, but their delivery indications are self-contained. This could mean something like a message waiting notification for a voice mail system, which was treated as an information service by J-STD-025, so it is excluded from CALEA intercept requirements.

(A) any alerting of incoming calls or messages;

(B) audible indications of incoming calls or messages (e.g., call waiting tone, message waiting tone, power alert/ring, distinctive alert/ring, recall alert/dial tone, or call forwarding reminder alert/ring, busy tone, or reorder tone);

It is not clear what is meant by recall dial tone. If this is the normal stutter dial tone, it is indicative of a particular call

processing state and does not indicate an incoming call. If this is the stutter dial tone applied upon going off-hook, it may indicate a message waiting (an information service). In neither case does this tone indicate an incoming call.

Busy tone does not indicate an incoming call. It is applied by the called end of a call which is not the intercept subject's equipment.

Reorder tone does not indicate an incoming call. It is applied by the called end of a call, which is not the intercept subject's equipment.

(C) visual indications of incoming calls or messages (e.g., lights to indicate call waiting); and

This requirement should only apply to individual line or call appearance lamp controls for the intercept subject's terminal. It should not apply to Direct Station Select/Busy Lamp Fields that are used to report on the line and station status for all members of a business group. (To do so would require a court order covering all of the persons belonging to the business group and by so doing, all of the individuals would be reported separately.)

(D) alphanumeric display information (e.g., messages sent to the terminal, calling number identification, or calling name identification).

This requirement is overly broad and would include any data communication service or information service that displayed alphanumeric information on a subscriber's terminal. This capability should not extend beyond call-related information, such as the calling number identification and calling name identification. However, it should be noted that this requirement would then be redundant with information reported in the J-STD-025 Termination message.